IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Vitaly Neyman et al.

Serial No.: 09/862,801

Filing Date: May 22, 2001

Examiner: Kambiz Zand

Art Unit: 2132

Title: SYSTEM AND METHOD FOR INCREASING HEURISTICS SUSPICION LEVELS IN ANALYZED COMPUTER CODE

Mail Stop AF
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

"EXPRESS MAIL
Express Mailing Label Number EV733640385 US

Date of Deposit

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to Mail Stop AF, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Willie Jiles
Willie Jiles

Dear Sir:

Dear Sir:

PRE-APPEAL BRIEF REQUEST FOR REVIEW

The following Pre-Appeal Brief Request for Review ("Request") is being filed in accordance with the provisions set forth in the Official Gazette Notice of July 12, 2005 ("OG Notice"). Pursuant to the OG Notice, this Request is being filed concurrently with a Notice of Appeal. The Applicants respectfully request reconsideration of the rejection of all claims in the Application.

REMARKS

In the prosecution of the present Application, the Examiner's rejections and assertions contain clear errors of law. Most notable of the legal errors present in the examination of the Application is a failure of the Final Office Action to establish a *prima facie* rejection of the claims in the application under 35 U.S.C§ 103. The Final Office Action rejected Claims 1-32 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,519,703 issued to Joyce ("*Joyce*") in view of an Alleged Admission of Prior Art (*AAPA*).[1] However, these rejections fail to meet the required *prima facie* standard for obviousness for at least the three reasons set forth below.

First, Independent Claim 1 is allowable because the proposed *Joyce-AAPA* combination fails to teach or suggest each of "selecting a fastest one of the malicious code detection methods"; "analyzing computer code for malicious code using the selected malicious code detection method", and "selecting a next fastest one of the malicious code detection methods." The Final Office Action acknowledged that *Joyce* did not disclose these limitations. *See* Final Office Action, Page 4. Rather, the Final Office Action relied on the AAPA to disclose these limitations. However, this is incorrect. The AAPA, Applicants' Specification section entitled "Description of the Related Art", simply does disclose the above limitations. Rather, the AAPA introduces the concept that "[d]ifferent hueristic detection methods may require different amounts of time and/or utilize varying amount of computer resources." Page 2 of Application. Clearly, such a disclosure does not disclose the above limitations. The Advisory Action of November 2, 2005, does not challenge that the AAPA fails to teach these limitations.

Second, Independent Claim 1 is allowable also because the proposed *Joyce-AAPA* combination fails to teach or suggest "*repeating the analyzing and determining steps* if the probability of accuracy is below a predetermined level." With regards to this limitation, the Final Office Action cites *Column* 2, lines 42-65 and the Abstract of *Joyce*. However, this is incorrect. In these sections, *Joyce* does not disclose *repeating the analyzing and determining steps*. Rather, *Joyce* describes a system in which data packets 22 undergo a hueristic analysis stage 16. Based upon the hueristic analysis stage 16, the data packets 22 are assigned a confidence level. If they have a "high-confidence," they are released to a traditional firewall rule base 12. If they have a "marginal-confidence," they are release into a more complex

[1] The AAPA cited in the Office Action is the section entitled "Description of the Related Art" in the Application.

firewall rules base 14. If they have a "poor-confience," they are shunted out of firewall 10A. In this portion of *Joyce*, no disclosure is made as to an *additional determination of a probability of accuracy of a result of an additional analysis.*

Third, Independent Claim 1 is allowable also because there is no motivation to combine *Joyce* with *AAPA*. The Final Office Action submitted the following alleged motivation:

> It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize AAPA's prior art disclosure in Joyce's Heuristic packet filter analysis in order to provide different methods based on Hueristic's logic based rules.

(Office Action, Page 4.) Applicants submit that this alleged motivation simply does not meet the required evidentiary threshold necessary for a *prima facie* motivation. As referenced above, the Final Office Action acknowledged that *Joyce* does not disclose "wherein at least some of the malicious code detection methods require different amounts of time to analyze for code, selecting a fastest one of the malicious code detection methods, analyzing computer code for malicious code using the selected malicious code detection method; selecting a next fastest one of the malicious code detection method." Office Action, Page 4. Accordingly, at a minimum, prior art references would need to suggest desirability in combining the above limitations with *Joyce*.

As described above, the Advisory Action of November 2, 2005, did not address the first of the above arguments (lack of a disclosure of "selecting a fastest one of the malicious code detection methods"; "analyzing computer code for malicious code using the selected malicious code detection method", and "selecting a next fastest one of the malicious code detection methods."). In response to the second argument (lack of a disclosure of "repeating the analyzing and determining steps if the probability of accuracy is below a predetermined level"), the Advisory Action pointed to a portion of *Joyce*, which states in pertinent part:

> In one embodiment, the shunted packets are subject to additional analysis and/or processing to determine the reason for the low confidence.

(Column 2, lines 55-57). Clearly, the "additional analysis" recited in the above passage does not engage in repeating the analyzing and determining steps, which includes "analyzing computer code for malicious code using the selected malicious code detection method" and "determining a probability of accuracy of a result of the analysis." Rather, the additional analysis simply determines the reason for a low confidence for the shunted packet.

In response to the third argument (lack of a motivation to combine *Joyce* with *AAPA*), the Advisory Action indicated (1) that "the Applicants' invention and the Joyce invention are within the same technological environment and fields of art" and (2) that "the motivation to combine such methods in Joyce are set forth in the limitation 'AV systems using heuristics logic may use self-educating techniques to improve performance.'" (taken from *AAPA*, page 1). Applicants submit that this alleged motivation still does not meet the required evidentiary threshold necessary for a *prima facie* motivation. First, the mere fact that two references are in a related field is clearly not a motivation to combine references. *See Ex Parte Kuo-Yu Chou,* Appeal No. 2005-1937 at page 10 (Bd. Pat. App. & Int. 2005). Second, the statement quoted from the AAPA clearly would not motivate one of ordinary skill in the art to make the proposed *Joyce-AAPA* combination because it mentions nothing about the desirability of the combination. *See* MPEP 2143.01. Particularly, the Final Office Action acknowledges that *Joyce* does not disclose "wherein at least some of the malicious code detection methods require different amounts of time to analyze for code, selecting a fastest one of the malicious code detection methods, analyzing computer code for malicious code using the selected malicious code detection method; selecting a next fastest one of the malicious code detection method." Office Action, Page 4. Accordingly, at a minimum, prior art references would need to suggest desirability in combining the above limitations with *Joyce*. The cited quote does not do that. Accordingly, the motivation to combine is still lacking.

Accordingly, Applicants maintain that Independent Claim 1 and its dependents, Claims 2-6, should be allowed. Independent Claims 7, 13, 19, 25, 26, 27, 28, 29, 30, 31, and 32 should also be allowed for analogous reasons as should their dependents, Claims 8-12, 14-18, and 20-24.

CONCLUSION

As a *prima facie* rejection has not been established against Applicants' claims, Applicants respectfully request a finding of allowance of all claims in the Application.

To the extent necessary, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of BAKER BOTTS L.L.P.

Respectfully submitted,
BAKER BOTTS L.L.P.
Attorneys for Applicants

Bradley P. Williams
Reg. No. 40,227

Dated: December 2, 2005

Correspondence Address:
Customer Number: **05073**